Pre-Hashing as a Cryptographic Tool for Securing Entrepreneurial Ideas

Jean Rendon, Clariandys Rivera, Afshin Gholamy, and Leobardo Valera

Abstract As cyberattacks grow more sophisticated, enhancing password security has become a critical challenge in modern authentication systems. This paper introduces a novel pre-hashing technique that strengthens password protection by applying a cryptographic hash function to user credentials before the standard hashing and storage process. The result is a dual-layered model that significantly increases resistance to brute-force, rainbow table, and shadow file attacks. We present the structure and implementation of this approach, demonstrating how it can be integrated into existing authentication frameworks. As a practical application, we explore how this method can be used to safeguard sensitive digital assets—particularly entrepreneurial ideas and intellectual property—by providing verifiable, tamper-resistant evidence of originality and ownership.

Jean Rendon
El Paso Community College
919 Hunter Dr
El Paso, TX 79915, USA
e-mail: jeanrendon@gmail.com

Clariandys Rivera
Centro de Gerencia y Liderazgo
Instituto de Estudios Superiores de Administración
Caracas, Venezuela
e-mail: clariandys.rivera@iesa.edu.ve

Afshin Gholamy
National University
9388 Lightwave Ave,
San Diego, CA 92123, USA
e-mail: agholamy@nu.edu

Leobardo Valera
El Paso Community College
919 Hunter Dr,
El Paso, TX 79915, USA
e-mail: lvalerav@epcc.edu

1 Background and Related Work

In recent years, digital security has become a key concern for businesses, especially for entrepreneurs who deal with valuable intellectual property (IP) [1]. Various methods, such as encryption and hashing, have been employed to protect sensitive information from unauthorized access [2]. Traditional cryptographic hash functions such as SHA-256 and SHA-512 are widely used to ensure data integrity and confidentiality [5, 6]. To better understand how hashing works, let's walk through how a raw password is stored in the shadow file of a Linux system.

Consider $x \in \Sigma^*$ a raw password, where $x \in \Sigma$ is a string of symbols. We encode it as a binary string:

$$B : \Sigma^* \to \{0,1\}^*$$

The function B converts any string of symbols into a string of 0's and 1's. Then, the system hashes the string $B(x)$:

$$H : \{0,1\}^* \to \{0,1\}^{512}$$

Finally, we convert the hashed string to a printable ASCII format using hexadecimal or Base64 encoding:

$$A : \{0,1\}^{512} \to \Sigma^*_{\text{ascii}}$$

We can summarize the process as a composition of functions:

$$\text{StoredHash}(x) = (A \circ H \circ B)(x)$$

The hackers obtain the shadow file by any means and read the Base64-encoded hash of the victim's password stored in the shadow file. They then apply the previously described process to a list of weak passwords they have collected (many of which are publicly available), hashing each one until the result matches the victim's stored Base64 string. The pre-hashing process adds two additional layers of protection, making it virtually impossible to decrypt the Base64-encoded string stored in the shadow file.

2 Pre-Hashing Protection

Pre-hashing involves transforming a piece of data into a fixed-size string of characters that adds an extra layer of security to the original data [3, 4]. This paper explores the benefits of pre-hashing and strives to demonstrate how this technique can add another extra layer of security against potential breaches, offering protection to innovators and their intellectual property.

Pre-hashing enhances data security by applying an additional transformation (such as encryption or an intermediary hash function) before the final hashing step, making it significantly more difficult to reconstruct the original data even if the initial hash is exposed. Pre-hashing introduces a two-tiered defense mechanism, enhancing the overall security posture.

$$\text{StoredHash}(x) = (A \circ H \circ B \circ P \circ B)(x)$$

where P is an additional pre-hash function that could be the same SHA-512 or a different cryptographic function.

The importance of multi-layered strategies in the context of digital data protection has been emphasized by researchers [6]. Pre-hashing and advanced encryption schemes are closely tied together and their joint application allow for the secure storage and retrieval of sensitive data without compromising its confidentiality [7].

2.1 Pre-hashing with Salt

The process of pre-hashing can be further strengthened by adding a unique salt (a random value added to the password before hashing) to each password before hashing. This prevents attackers from using precomputed hash tables, also known as rainbow tables, to reverse-engineer passwords.

We compare three password protection techniques—plain storage, pre-hashing without salt, and pre-hashing with salt—using key criteria such as storage and retrieval complexity, security strength, and resistance to password-cracking attempts.

- **No Pre-hashing (Plaintext Storage):** This method offers zero security, weak performance and fast and easy exploitation. Passwords are directly exposed upon breach.
- **Pre-hashing without Salt:** This approach provides moderate security and relatively fast cracking performance which renders the data to be vulnerable to rainbow table and brute force attacks due to deterministic hashing.

2.2 Pre-Hashing Test and Evaluation

To validate the proposed method, pre-hashing with salt was tested on a common weak password, “123456.” Despite being widely used, the pre-hashing with salt method successfully prevented this password from being compromised. The results confirm that while pre-hashing with salt introduces slightly increased computational overhead, it provides dramatically stronger protection, making it the recommended method for securing passwords, ensuring the best balance between performance and security.

3 Entrepreneurial Protection Using Pre-Hashing

Cryptographic techniques such as pre-hashing with a salt act as a safeguard for the integrity and confidentiality of entrepreneurial ideas and intellectual properties [8]. Pre-hashing applies a hashing function to an idea before it is shared or stored, which guarantees that data remains unchanged and verifiable at any time [7, 9]. This allows entrepreneurs to demonstrate the originality of their idea while preserving its confidentiality [7]. One of the most common applications of pre-hashing for entrepreneurial protection is in the documentation and registration of business ideas and patenting. This serves as proof that the idea or patent existed at a certain point in time without having to reveal the full details [10, 11]. A natural extension of pre-hashing in entrepreneurial ideas protection is its integration with blockchain technology. Storing these ideas as hashes on blockchains ensures a tamper-proof, timestamped record that can be used as evidence in case of legal disputes [12, 13].

While pre-hashing offers significant advantages in securing entrepreneurial ideas, it is not without its limitations and challenges. One major drawback is that pre-hashing does not allow refinement or iteration of the idea after they have been hashed and stored [14]. Additionally, pre-hashing doesn't prevent other entrepreneurs from independently generating the same or a similar idea. This requires entrepreneurs to consider patenting, copyrighting, or other forms of legal protection as proof of originality [15].

4 Challenges and Solutions in Cybersecurity for Entrepreneurs

Entrepreneurs often lack the resources or awareness for cybersecurity. Perceived low risk, limited budgets, and complexity of tools prevent adoption. Cyberattacks can lead to financial and operational damage. Pre-hashing offers an accessible starting point. A layered strategy, including training and good practices, is essential [15, 16].

5 Conclusion

Pre-hashing, particularly with salt, enhances security against modern attack vectors and provides verifiable proof of ownership. The paper advocates wider adoption of pre-hashing, especially when combined with legal protections and blockchain technology. Entrepreneurs can use this to defend their intellectual property and sensitive digital assets in a secure, confidential, and scalable manner.

Acknowledgments

The authors would like to thank the Centro de Gerencia y Liderazgo at the Instituto de Estudios Superiores de Administración and Desert Image (Diagnostic Imaging and Radiology in El Paso, TX) for their institutional support, which provided the time and flexibility necessary to carry out this research. We are also deeply grateful to the Theoretical Research and its Application in Computer Science in The University of Texas at El Paso (TRACS) group for granting access to its research lab facilities—an essential contribution to the development of this article.

We also extend our sincere thanks to the School of Arts, Letters and Sciences at National University for their ongoing support throughout this project. In particular, we are grateful to the Department of Mathematics and Natural Sciences for their academic guidance, access to resources, and the intellectually stimulating environment they provided. Their commitment to fostering research and inquiry has been instrumental in bringing this study to fruition.

References

1. D. Boneh, H. Corrigan-Gibbs, and S. Schechter, "Balloon hashing: A memory-hard function providing provable protection against sequential attacks," *IACR Cryptology ePrint Archive*, 2016.
2. Y. Zohar and Y. Hillel, "Prehashing passwords for secure authentication," *Journal of Cryptographic Engineering*, Vol. 7, No. 2, 2016, pp. 85–99.
3. A. Miller and S. Thompson, *Advanced Techniques in Cybersecurity: From Hacking to Protection*, Springer, Berlin, 2017.
4. C. Jin, X. Wang, and Y. Zhang, "Exploring pre-hashing algorithms for password protection in distributed systems," *IEEE Transactions on Information Forensics and Security*, Vol. 14, No. 3, 2019, pp. 593–607.
5. M. Bauer, M. Schwab, and W. Zhang, "Enhancing data protection in modern systems with cryptographic methods," *Information Security Journal: A Global Perspective*, Vol. 33, No. 4, 2020, pp. 45–59.
6. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., Wiley, New York, 1996.
7. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1997.
8. R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley, Hoboken, New Jersey, 2020.
9. R.L. Rivest, The MD5 message-digest algorithm. RFC 1321 (1992).
10. C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, Vol. 28, No. 4, 1949, pp. 656–715.
11. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. 22, No. 6, 1976, pp. 644–654.
12. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed., Springer, New York, 2015.
13. M. Bellare and G. Neven, "Transitive encryption and its applications," *Journal of Cryptology*, Vol. 21, No. 3, 2008, pp. 337–374.
14. P. Rogaway and T. Shrimpton, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, Berlin, 2009.

15. C. D. Díaz Jiménez, E. Ariza Rodríguez, and M. Y. Ruiz Moncada, “La ciberseguridad en las pymes,” *Journal of Cybersecurity in SMEs*, 2023.
16. F. X. J. Pruna, P. V. Y. Jeada, and J. L. C. Jumbo, “Análisis de las características del sector microempresarial en Latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información,” *Revista Científica ECOCIENCIA*, Vol. 7, No. 1, 2020, pp. 1–26.